

POLYNOMIAL-VALUE SIEVING AND RECURSIVELY-FACTORABLE POLYNOMIALS

JONATHAN BURNS

ABSTRACT. We identify a recursive structure among factorizations of polynomial values into two integer factors. Polynomials for which this recursive structure characterizes all non-trivial representations of integer factorizations of the polynomial values into two parts are here called recursively-factorable polynomials. In particular, we prove that $n^2 + 1$ and the prime-producing polynomials $n^2 + n + 41$ and $2n^2 + 29$ are recursively-factorable.

For quadratics, we prove that this recursive structure is equivalent to a Diophantine identity involving the product of two binary quadratic forms. We show that this identity may be transformed into geometric terms, relating each integer factorization $an^2 + bn + c = pq$ to a lattice point of the conic section $aX^2 + bXY + cY^2 + X - nY = 0$, and vice versa.

1. INTRODUCTION

The sieve of Eratosthenes is the oldest and most well-known of the integer sieves, and is used to find all the primes up to a given limit N . The sieve begins with the list of integers $L = (2, 3, \dots, N)$ and proceeds iteratively by marking the smallest number on the list as prime and removing it along with its multiples from the list. The smallest number still left on the list is marked as prime and the procedure continues until the list is empty.

Algorithmically, the sieve of Eratosthenes both identifies the prime numbers in the list and yields a unique prime factorization for the composite numbers through multiple presentations of each polynomial value as product of two integers. In other words, each value $F(n) = n$ in the sequence $L = (F(2), F(3), \dots, F(N))$ is presented as the factorization presentation $F(n) = pq$ for each $p \mid F(n)$. If however F is an arbitrary polynomial with integer coefficients and $p \mid F(n)$, then $p \mid F(n + kp)$ for each $k \in \mathbb{Z}$ too. Hence, the algorithm can be generalized to include other polynomials at the cost of missing some of the factorization presentations. Fortunately, the situation can be improved by taking both factors of each composite $F(n)$ into consideration, i.e., if $F(n) = pq$ is marked as being divisible by p then all $F(n + kq)$ where $k \in \mathbb{Z}$ can be marked as being divisible by q as well.

To keep track of all the factorization presentations, it suffices to record the initial value along with the sequence of quotients for the multiples of the factors, e.g., if $F(x_1) = 1 \cdot p_1$, $F(x_1 + x_2 p_1) = p_1 p_2$ and $F(x_1 + x_2 p_1 + x_3 p_2) = p_2 p_3$ then the factorization presentation can be reconstructed from the sequence (x_1, x_2, x_3) . This method of sieving the polynomial values for integer factorizations is expressed in Theorem 2.1, and holds in the context of multivariate polynomials as well. Section 3 introduces a family of polynomials called *recursively-factorable polynomials* for which the collection of factorization presentations corresponding to the sequences $\{(x_1, \dots, x_m) \in \mathbb{Z}^m\}_{m=1}^\infty$ yield the unique prime factorization for each value of F via presentations $F(n) = pq$ for each $p \mid F(n)$.

DEPARTMENT OF MATHEMATICS & STATISTICS, UNIVERSITY OF SOUTH FLORIDA, 4202 FOWLER AVE., TAMPA, FL 33620-5700, USA

E-mail address: jtburns@mail.usf.edu.

In general, recursively-factorable polynomials are rare, but there are some noteworthy instances. Particularly, the *Euler-like* and *Legendre-like* prime producing polynomials of the form $n^2 + n + c$ for $c \in \{2, 3, 5, 11, 17, 41\}$ and $2n^2 + c$ for $c = \{3, 5, 11, 29\}$, respectively, and Landau's $n^2 + 1$ are recursively-factorable. The sieve of Eratosthenes verifies that the line n is also recursively-factorable, but we presently focus on recursively-factorable quadratic equations.

In Section 4, we introduce an identity which presents the factorization of a quadratic polynomial value as the product of two binary quadratic forms (Theorem 4.3) and show that this identity associates all the factorization presentations of the aforementioned polynomial-value sieving integer sequences with the set $\Gamma_a := \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z}) \mid \alpha\delta - a\beta\gamma = 1 \right\}$. For monic quadratics, $a = 1$ and the factorization presentations correspond to the transvection generators of $\Gamma_1 = \text{SL}_2(\mathbb{Z})$ (Corollary 4.10).

In Section 5, a bijection is established (Theorem 5.1) between Γ_a and the set \mathcal{L}_a of lattice point solutions $(X, Y) \in \mathbb{Z}^2$ for the conic sections $aX^2 + bXY + cY^2 + X - nY = 0$ with $a, b, c, n \in \mathbb{Z}$, showing that \mathcal{L}_a does not depend on b, c , or n . Following the mappings in Figure 1, each lattice point (X, Y) of the conic section is associated with an element of Γ_a and gives a factorization presentation for $F(n) = an^2 + bn + c$. If a factorization presentation $F(n) = pq$ has a corresponding integer sequence (x_1, \dots, x_m) then there is a matching element of Γ_a which corresponds to a lattice point solution of the conic section.

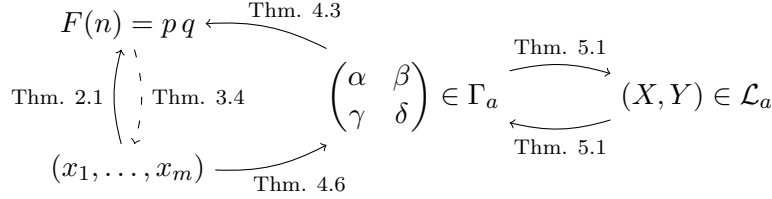


FIGURE 1. Relationships between factorization presentations $an^2 + bn + c = pq$, the polynomial-value sieving sequence (x_1, \dots, x_m) , the set of 2×2 integers matrices Γ_a , and the set of lattice point solutions \mathcal{L}_a to the conic section $aX^2 + bXY + cY^2 + X - nY = 0$.

2. POLYNOMIAL-VALUE SIEVING

Theorem 2.1. Let \mathcal{R} be a commutative ring with identity. For any polynomial $F \in \mathcal{R}[x]$ of degree d , there exists a sequence of multivariate polynomials $\{f_m(x_1, \dots, x_m)\}_{m=0}^\infty$ such that $f_m(x_1, \dots, x_m) \in \mathcal{R}[x_1, \dots, x_m]$ and

$$(1) \quad F\left(\sum_{k=1}^m x_k f_{k-1}(x_1, \dots, x_{k-1})\right) = f_{m-1}(x_1, \dots, x_{m-1}) f_m(x_1, \dots, x_m)$$

where $f_0 = 1$, $f_1(x_1) = F(x_1)$, and

$$f_m = f_{m-2} + x_m \sum_{j=1}^d \frac{1}{j!} \left(x_m \frac{f_{m-1}}{f_{m-2}} \right)^{j-1} \frac{\partial^j f_{m-1}}{\partial x_{m-1}^j}$$

for $m \geq 2$ with the convention that f_m is shorthand for $f_m(x_1, \dots, x_m)$.

Proof. Since $F(x_1 f_0) = f_0 f_1(x_1)$ represents the trivial factorization, the statement is initially true and we proceed by induction on m . Let $D^{(j)}$ be the j th order Hasse derivative and $D_x^{(j)} = \frac{1}{j!} \frac{d^j}{dx^j}$ be the j th order Hasse derivative with respect to the intermediate x . Applying $D_{x_{m-1}}^{(j)}$ to both sides of $F\left(\sum_{k=1}^{m-1} x_k f_{k-1}\right) = f_{m-2} f_{m-1}$ gives

$$(2) \quad (D^{(j)} F) \left(\sum_{k=1}^{m-1} x_k f_{k-1} \right) \cdot f_{m-2}^j = f_{m-2} \cdot D_{x_{m-1}}^{(j)} f_{m-1}.$$

Using the Taylor series expansion for F ,

$$(3) \quad \begin{aligned} F \left(\sum_{k=1}^m x_k f_{k-1} \right) &= \sum_{j=0}^d (D^{(j)} F) \left(\sum_{k=1}^{m-1} x_k f_{k-1} \right) \cdot (x_m f_{m-1})^j \\ &= F \left(\sum_{k=1}^{m-1} x_k f_{k-1} \right) + (x_m f_{m-1}) \sum_{j=1}^d (D^{(j)} F) \left(\sum_{k=1}^{m-1} x_k f_{k-1} \right) \cdot (x_m f_{m-1})^{j-1} \\ &= f_{m-1} \cdot \left(f_{m-2} + x_m \sum_{j=1}^d (D^{(j)} F) \left(\sum_{k=1}^{m-1} x_k f_{k-1} \right) \cdot (x_m f_{m-1})^{j-1} \right) \end{aligned}$$

which gives a definition for $f_m(x_1, \dots, x_m) \in \mathcal{R}[x_1, \dots, x_m]$. Substituting (2) into (3) yields

$$(4) \quad f_m = f_{m-2} + x_m \sum_{j=1}^d \left(x_m \frac{f_{m-1}}{f_{m-2}} \right)^{j-1} D_{x_{m-1}}^{(j)} f_{m-1}. \quad \square$$

Remark 2.2. For $F(z) = \sum_{i=0}^d a_i z^i$, taking $j = d$ in equation (2) gives

$$\frac{D_{x_{m-1}}^{(d)} f_{m-1}}{(f_{m-2})^{d-1}} = a_d$$

for all $d \geq 1$. So for $d = 2$, Theorem 2.1 expresses f_m as

$$(5) \quad f_m = f_{m-2} + x_m \frac{\partial f_{m-1}}{\partial x_{m-1}} + a_2 x_m^2 f_{m-1}.$$

Remark 2.3. For each sequence (x_1, \dots, x_m) , if $x_i = x_{i_a} + x_{i_b}$ then

$$(6) \quad f_m(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_m) = f_{m+2}(x_1, x_2, \dots, x_{i-1}, x_{i_a}, 0, x_{i_b}, x_{i+1}, \dots, x_m).$$

Moreover if $(x_1, \dots, x_m) \in \mathbb{Z}^m$, then there exists f_M such that

$$f_m(x_1, \dots, x_m) = f_M(z_1, \dots, z_M)$$

where $z_i \in \{-1, 0, 1\}$ and $M = \sum_{j=1}^m 2|x_j| - 1$.

Example 2.4. Let $F(x) = 3x^2 + 5x + 11$. We compute $f_3(2, -1, 4)$ as follows:

$$\begin{aligned}
f_0 &= 1 \\
f_1(2) &= \frac{F(2 \cdot 1)}{1} = \frac{F(2)}{1} = 33 \\
f_2(2, -1) &= \frac{F(2 + (-1) \cdot 33)}{33} = \frac{F(-31)}{33} = 83 \\
f_3(2, -1, 4) &= \frac{F(-31 + 4 \cdot 83)}{83} = \frac{F(301)}{83} = 3293
\end{aligned}$$

This gives $F(301) = 273319 = 83 \times 3293$. One can also verify that

$$f_3(2, -1, 4) = f_{11}(1, 0, 1, -1, 1, 0, 1, 0, 1, 0, 1).$$

3. RECURSIVELY-FACTORABLE POLYNOMIALS

Theorem 2.1 provides a means of factoring the values of a polynomial F into two integers, but these presentations may not represent the full solution set $\{(n, p, q) \in \mathbb{Z}^3 : F(n) = pq\}$. For example when $F(n) = n^2 + n + 7$, the integer factorization $F(1) = 3 \cdot 3$ cannot be presented via Theorem 2.1, i.e., there does not exist a finite sequence of integers (x_1, x_2, \dots, x_m) for which $f_m = 3$, $f_{m-1} = 3$, and $\sum_{k=1}^m x_k f_{k-1} = 1$. Proof of this fact is shown in Remark 4.8.

By contrast, Lemma 3.5 provides the existence of a family of polynomials \mathcal{F} for which the prime integer factorization of each value of $F \in \mathcal{F}$ can be reconstructed from the presentations of Theorem 2.1. Theorem 3.4 shows that this family of polynomials contains the recursively-factorable polynomials characterized by the following property.

Definition 3.1. Let F be a polynomial with integer coefficients. If for each integer factorization presentation $F(n) = pq$ there exists an $r \in \mathbb{Z}$ such that $|F(r)| < |F(n)|$ and $r \equiv n \pmod{|p|}$ or $r \equiv n \pmod{|q|}$, then n is said to satisfy the *recursively-factorable criterion* for F . If each $n \in \mathbb{Z}$ satisfies the recursively-factorable criterion for F , then the polynomial F is said to be *recursively-factorable*.

Remark 3.2. Recursively-factorable polynomials are irreducible over \mathbb{Z} . If not then $F(n) = 0$ for some $n \in \mathbb{Z}$, but the non-trivial factorization $0 = 0 \cdot p_0$ has no associated $r \equiv n \pmod{|p_0|}$ such that $|F(r)| < |F(n)| = 0$ for any $p_0 \in \mathbb{Z}$.

Lemma 3.3. Let F be a polynomial and $G(n) = \pm F(n - h)$ for some $h \in \mathbb{Z}$. If F is recursively-factorable, then so is G .

Proof. Suppose that $G(n) = \pm F(n - h) = p_0 p_1$ is a non-trivial factorization. Since F is recursively-factorable, we may assume without loss of generality that there exists $q \in \mathbb{Z}$ such that $|F(r)| < |F(n - h)|$ where $r = (n - h) - q p_0$. Thus $|G(r + h)| < |G(n)|$ and $r + h = n - q p_0 \equiv n \pmod{|p_0|}$, so we may conclude that G is recursively-factorable. \square

Theorem 3.4. If F is recursively-factorable then, for each $n \in \mathbb{Z}$ and $p \in \mathbb{N}$ such that $p \mid F(n)$, there exists a finite sequence of integers (x_1, x_2, \dots, x_m) such that

$$(7) \quad n = \sum_{k=1}^m x_k f_{k-1}(x_1, \dots, x_{k-1}) \quad \text{and} \quad p = |f_m(x_1, \dots, x_{m-1}, x_m)|.$$

Proof. Fix $n \in \mathbb{Z}$. If $p = 1$ or $|F(n)|$ then the sequence (n) gives the presentation $F(n) = F(n \cdot f_0) = f_0 f_1(n) = 1 \cdot F(n)$. Thus it is sufficient to consider the case where $F(n)$ is a composite integer with a non-trivial factorization $F(n) = p_1 p_0$ such that $p = |p_0|$.

Let $R = \{r \in \mathbb{Z} : r \equiv n \pmod{|p_0|} \text{ or } r \equiv n \pmod{|p_1|}\}$. Since F is recursively-factorable, there exists an $r \in R$ such that $|F(r)| < |F(n)|$. Moreover there is an $r_1 \in R$ such that $|F(r_1)| \leq |F(r)|$ for all $r \in R$. Set $p_* = p_0$ or p_1 so that $r_1 \equiv n \pmod{|p_*|}$. It follows that $n = q_1 p_* + r_1$ and $F(r_1) = p_2 p_*$ for some $q_1, p_2 \in \mathbb{Z}$. If $|p_2| = 1$, then $F(r_1) = p_2 p_*$ represents a trivial factorization and the sequence (r_1, q_1) yields the presentation

$$(8) \quad F(n) = F(r_1 p_2 + q_1 p_*) = f_1(r_1) f_2(r_1, q_1).$$

If $|p_2| \neq 1$, then $F(r_1) = p_* p_2$ represents a non-trivial factorization, and by the minimality of our choice of r_1 relative to all other $r \in R$ there exists an r_2 which minimizes $|F(r_2)| < |F(r_1)|$ over all $r_2 \equiv r_1 \pmod{|p_2|}$, i.e., $r_1 = q_2 p_2 + r_2$ for some $q_2 \in \mathbb{Z}$.

We may continue in this fashion until we obtain the trivial integer factorization $F(r_{m-1}) = p_{m-1} p_m$ where $|p_m| = 1$, produced from a finite sequence of factors $(p^*, p_2, \dots, p_{m-1}, p_m)$, quotients $(q_1, q_2, \dots, q_{m-1})$ and remainders $(r_1, r_2, \dots, r_{m-1})$ such that $r_k = q_{k+1} p_{k+1} + r_{k+1}$ and $F(r_k) = p_k p_{k+1}$ for each $2 \leq k \leq m-1$. Starting with $p_m = 1$ and $F(r_{m-1}) = p_{m-1} p_m$ we may reverse this sequence to obtain n and p as follows:

$$p_{m-1} = \frac{F(r_{m-1})}{p_m} = \frac{F(r_{m-1})}{f_0} = f_1(r_{m-1}),$$

$$p_{m-2} = \frac{F(r_{m-2})}{p_{m-1}} = \frac{F(r_{m-1} + q_{m-1} p_{m-1})}{p_{m-1}} = \frac{F(r_{m-1} f_0 + q_{m-1} f_1(r_{m-1}))}{f_1(r_{m-1})} = f_2(r_{m-1}, q_{m-1}).$$

More generally

$$p_k = f_{m-k}(r_{m-1}, q_{m-1}, q_{m-2}, \dots, q_{k+1})$$

for $2 \leq k \leq m-2$ and $p_* = f_{m-1}(r_{m-1}, q_{m-1}, \dots, q_2)$.

Therefore the integer sequence $(r_{m-1}, q_{m-1}, \dots, q_1)$ gives the presentation

$$\begin{aligned} F(n) &= F\left(r_{m-1} f_0 + q_{m-1} f_1(r_{m-1}) + \sum_{k=3}^m q_{m-k+1} f_{k-1}(r_{m-1}, q_{m-1}, \dots, q_{m-k+2})\right) \\ &= f_{m-1}(r_{m-1}, q_{m-1}, \dots, q_2) f_m(r_{m-1}, q_{m-1}, \dots, q_2, q_1), \end{aligned}$$

and $p = |f_m(r_{m-1}, q_{m-1}, \dots, q_1)|$. □

The proof of Theorem 3.4 starts with an integer factorization $F(n_0) = p_1 p_0$ and constructs a sequence of factorizations $F(n_1) = p_1 p_2$, $F(n_2) = p_2 p_3, \dots$ such that $|F(n_0)| > |F(n_1)| > |F(n_2)| \dots$ until a prime number $F(n_m)$ with the trivial factorization $F(n_m) \cdot 1$ is reached. In this way prime-producing polynomials, which contain a large interval of consecutive prime values, make good candidates for having the recursively-factorable property.

In 1772, Euler [10] discovered that the polynomial $n^2 - n + 41$ produces prime numbers for $n \in [-39, 40]$, and later Legendre [19] noted that both $n^2 + n + 17$ and $n^2 + n + 41$ are prime for $n \in [-16, 15]$ and $n \in [-40, 39]$, respectively. Le Lionnais considered polynomials of the type $n^2 + n + \varepsilon$ in general, which he called Euler-like polynomials [20], and integers ε for which $n^2 + n + \varepsilon$ is prime for $n = 0, 1, \dots, \varepsilon - 2$ have come to be known as *lucky numbers of Euler*.

Rabinowitz [25] proved that ε is a lucky number of Euler if and only if the field $\mathbb{Q}(\sqrt{1 - 4\varepsilon})$ has class number 1. From this, Heegner [17] and Stark [28] showed that there are exactly six lucky numbers of Euler, namely 2, 3, 5, 11, 17, and 41.

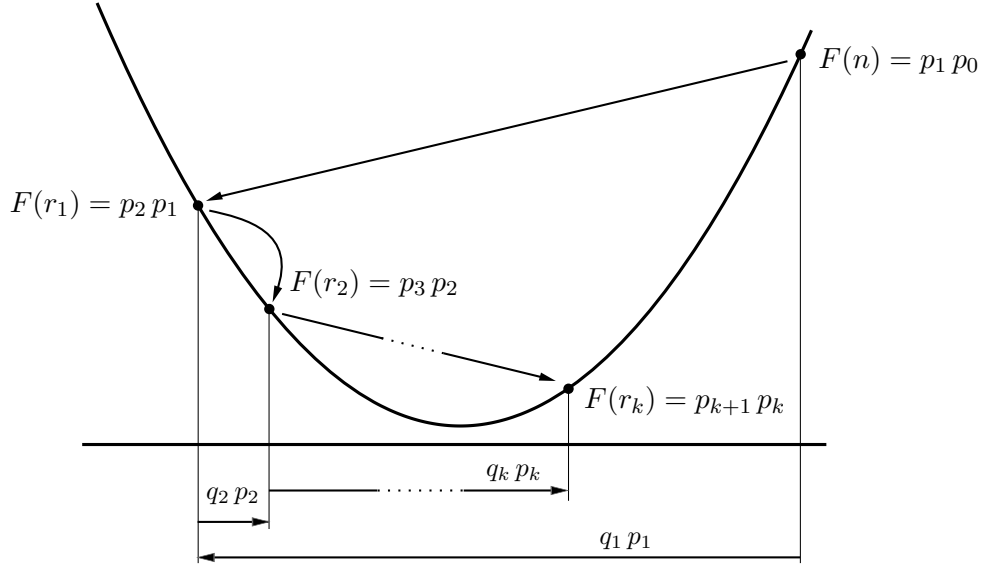


FIGURE 2. Sequence of decreasing values of F used to compute x_1, x_2, \dots, x_m in $f_m(x_1, x_2, \dots, x_m)$.

Legendre [19] explored other types of prime-producing quadratics such as $2n^2 + \lambda$ which is prime when $\lambda = 29$ for $n = 0, 1, \dots, 28$. Akin to the Euler-like polynomials, these quadratics give primes for $n = 0, 1, \dots, \lambda - 1$ for prime λ if and only if $\mathbb{Q}(\sqrt{-2\lambda})$ has class number 2 [12, 21]. Baker [2] and Stark [29] found that the only such λ are 3, 5, 11, and 29.

As seen in Lemma 3.5, Euler-like and Legendre-like prime-producing quadratics are indeed recursively-factorable. Further discussion of prime-producing quadratics can be found in [22, 26].

Lemma 3.5. The following quadratics (and their horizontal shifts) are recursively-factorable:

- (i) $n^2 + c$ where $c \in \{1, 2\}$,
- (ii) $n^2 + n + c$ where $c \in \{1, 2, 3, 5, 11, 17, 41\}$
- (iii) $2n^2 + c$ where $c \in \{1, 3, 5, 11, 29\}$,
- (iv) $2n^2 + 2n + c$ where $c \in \{1, 2, 3, 7, 19\}$,
- (v) $3n^2 + c$ where $c = 2$,
- (vi) $3n^2 + 3n + c$ where $c \in \{1, 2, 5, 11, 23\}$,
- (vii) $4n^2 + c$ where $c \in \{1, 3, 7\}$, and
- (viii) $4n^2 + 4n + c$ where $c \in \{2, 3, 5\}$.

Proof. We claim that if F is one of these polynomials and all the values within a suitably large interval $I_{\hat{n}}$ are known to satisfy the recursively-factorable criterion for F , then the remaining values outside of $I_{\hat{n}}$ also satisfy the recursively-factorable criterion.

Supposing $F(n) = an^2 + bn + c$ is one of the polynomials in cases (i)-(viii), F is a positive parabola having a minimum at either $n = 0$ or $n = -\frac{1}{2}$. Furthermore the values $F(n) = F(-n - \frac{b}{a})$ for all $n \in \mathbb{Z}$, so if n satisfies the recursively-factorable criterion then so does $-n - \frac{b}{a}$. Also note that $|F(m)| < |F(n)|$ for $m \in I_n = (\min\{-n - \frac{b}{a}, n\}, \max\{-n - \frac{b}{a}, n\})$.

For cases (i)-(vi), define \hat{n} such that $|2n + \frac{b}{a}| > \lfloor \sqrt{F(n)} \rfloor$ for each $n \geq \hat{n}$. Given that for each factorization presentation $F(n) = pq$ either $p \leq \lfloor \sqrt{F(n)} \rfloor$ or $q \leq \lfloor \sqrt{F(n)} \rfloor$, for $n \geq \hat{n}$ there exists

a $k \in \mathbb{Z}$ such that either $n - kp \in I_{\hat{n}}$ or $n - kq \in I_{\hat{n}}$. Thus if we can verify that the values within $I_{\hat{n}}$ satisfy the recursively-factorable criterion, then so do the values greater than \hat{n} (and symmetrically the values less than $-\hat{n} - \frac{b}{a}$), i.e., F is recursively-factorable. In cases (vii) and (viii) we use a sharper approximation of $\min\{p, q\}$ than $\lfloor \sqrt{F(n)} \rfloor$ to determine \hat{n} , but the idea is the same.

In cases (i), (iii), (v), and (vii), $F(n)$ is prime (or 1) for $n \in [1 - c, c - 1]$ and $c \mid F(\pm c)$ which means $c \mid F(0) = c$, so the recursively-factorable condition is satisfied for $n \in [-c, c]$. Similarly, $F(n)$ is prime (or 1) for $n \in [1 - c, c - 2]$ in cases (ii), (iv), (vi), and (viii). The recursively-factorable condition is satisfied for $-c$, $c - 1$, and c since $c \mid F(-c), F(c - 1), F(c)$ and $F(0) = F(-1) = c$. Hence for all cases (i)-(viii) the recursively-factorable criterion is satisfied for $n \in [-c, c]$.

Case (i): For $F(n) = n^2 + c$ with $c \in \{1, 2\}$, $\hat{n} = \lfloor \sqrt{\frac{c}{3}} \rfloor = 0$ and $I_{\hat{n}} = [0] \subset [-c, c]$.

Case (ii): For $n^2 + n + c$ with $c \in \{1, 2, 3, 5, 11, 17, 41\}$, $I_{\hat{n}} = \left[-\left\lfloor -\frac{1}{2} + \sqrt{\frac{4c-1}{12}} \right\rfloor - 1, \left\lfloor -\frac{1}{2} + \sqrt{\frac{4c-1}{12}} \right\rfloor \right]$ and yields the respective $I_{\hat{n}}$ intervals corresponding to each c : $[-1, 0] \subseteq [-1, 1]$, $[-1, 0] \subseteq [-2, 2]$, $[-1, 0] \subseteq [-3, 3]$, $[-1, 0] \subseteq [-5, 5]$, $[-2, 1] \subseteq [-11, 11]$, $[-2, 1] \subseteq [-17, 17]$, and $[-4, 3] \subseteq [-41, 41]$.

Case (iii): For $F(n) = 2n^2 + c$ with $c \in \{1, 3, 5, 11, 29\}$, $I_{\hat{n}} = [-\lfloor \sqrt{\frac{c}{2}} \rfloor, \lfloor \sqrt{\frac{c}{2}} \rfloor]$ which gives the respective intervals: $[0] \subseteq [-1, 1]$, $[-1, 1] \subseteq [-3, 3]$, $[-1, 1] \subseteq [-5, 5]$, $[-2, 2] \subseteq [-11, 11]$, and $[-3, 3] \subseteq [-29, 29]$.

Case (iv): Let $F(n) = 2n^2 + 2n + c$ with $c \in \{1, 2, 3, 7, 19\}$, $I_{\hat{n}} = \left[-\left\lfloor \frac{\sqrt{2c-1}-1}{2} \right\rfloor - 1, \left\lfloor \frac{\sqrt{2c-1}-1}{2} \right\rfloor \right]$ which gives the respective intervals: $[0] \subseteq [-1, 1]$, $[0] \subseteq [-2, 2]$, $[0] \subseteq [-3, 3]$, $[-1, 1] \subseteq [-7, 7]$, and $[-2, 2] \subseteq [-19, 19]$.

Case (v): Let $F(n) = 3n^2 + 2$, then $I_{\hat{n}} = [0] \subseteq [-2, 2]$.

Case (vi): Let $F(n) = 3n^2 + 3n + c$ with $c \in \{1, 2, 5, 11, 23\}$, $I_{\hat{n}} = \left[-\left\lfloor \frac{\sqrt{4c-3}-1}{2} \right\rfloor - 1, \left\lfloor \frac{\sqrt{4c-3}-1}{2} \right\rfloor \right]$ which gives the respective intervals: $[-1, 0] \subseteq [-1, 1]$, $[-1, 0] \subseteq [-2, 2]$, $[-2, 1] \subseteq [-5, 5]$, $[-3, 2] \subseteq [-11, 11]$, and $[-5, 4] \subseteq [-23, 23]$.

Case (vii): Let F be of the form $4n^2 + c$ with $c \in \{1, 3, 7\}$. We claim that if $F(n) = pq$ where $p \leq q$ is an integer factorization presentation, then $p < 2n$. Observe that $p = 2n + 1$ implies that $q \geq 2n + 1$ and

$$4n^2 + 4n + 1 = (2n + 1)^2 \leq pq = F(n) = 4n^2 + c \implies 4n + 1 \leq c$$

and is a contradiction for $n > c$. Similarly, for $p = 2n$ and $q \geq 2n + 1$,

$$4n^2 + 2n = 2n(2n + 1) \leq pq = F(n) = 4n^2 + c \implies 2n \leq c$$

and is also contradiction for $n > c$. Clearly $q \neq 2n$ since $4n^2 + c = F(n) \neq pq = (2n)^2 = 4n^2$. Thus we are guaranteed that $2n > p$ and there exists an $r \in (1 - n, n - 1)$ such that $r \equiv n \pmod{p}$.

Case (viii): Let F be of the form $4n^2 + 4n + c$ with $c \in \{2, 3, 5\}$. As in case (vii), we show that $p < 2n$ for each integer factorization presentation $F(n) = pq$ where $p \leq q$. First notice that taking $p = 2n + 2$ and $q \geq 2n + 2$ leads to

$$4n^2 + 8n + 4 = (2n + 2)^2 \leq pq = F(n) = 4n^2 + 4n + c \implies 4n + 4 \leq c$$

and is a contradiction for $n > c$. Likewise, taking $p = 2n + 1$ and $q \geq 2n + 2$ gives

$$4n^2 + 6n + 2 = (2n + 1)(2n + 2) \leq pq = F(n) = 4n^2 + 4n + c \implies 2n + 2 \leq c$$

	$c \leq 5000$
$n^2 - c$	2, 3, 6, 7, 11, 14, 23, 38, 47, 62, 83, 167, 227, 398
$n^2 + n - c$	1, 3, 4, 5, 7, 8, 9, 10, 13, 14, 15, 17, 18, 19, 22, 23, 25, 27, 28, 33, 37, 39, 43, 45, 49, 53, 59, 67, 69, 73, 75, 79, 85, 87, 93, 103, 109, 113, 115, 127, 129, 139, 153, 163, 169, 179, 193, 199, 205, 213, 235, 269, 283, 313, 337, 349, 373, 385, 409, 469, 499, 619, 643, 655, 763, 829, 865, 883, 997, 1063, 1555
$2n^2 - c$	1, 3, 5, 7, 11, 13, 15, 19, 21, 29, 31, 35, 37, 47, 55, 61, 67, 69, 79, 91, 101, 103, 133, 139, 157, 159, 181, 199, 229, 283, 439, 571, 643, 661, 1069
$2n^2 + 2n - c$	1, 2, 3, 5, 6, 7, 9, 10, 11, 14, 15, 17, 21, 23, 26, 27, 29, 35, 38, 41, 43, 53, 63, 65, 71, 81, 83, 86, 107, 113, 146, 149, 173, 185, 191, 215, 218, 223, 251, 317, 323, 371, 413, 491, 743, 833
$3n^2 - c$	1, 2, 5, 10, 14, 29, 46, 106, 149
$3n^2 + 3n - c$	1, 2, 3, 4, 5, 7, 8, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 55, 59, 65, 67, 79, 89, 95, 97, 107, 119, 131, 157, 163, 173, 199, 229, 257, 275, 317, 325, 457, 479, 635, 637, 1379
$4n^2 - c$	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 33, 41, 47, 59, 83, 107, 167, 227, 563
$4n^2 + 4n - c$	1, 2, 3, 5, 6, 7, 10, 11, 13, 19, 21, 22, 27, 31, 37, 43, 46, 51, 61, 67, 82, 85, 115, 127, 163, 166, 226, 277, 397

TABLE 1. Recursively-factorable polynomials with real roots.

and again is a contradiction for $n > c$. With $p = 2n + 1$ and $q = 2n + 1$, $4n^2 + 4n + c = F(n) \neq pq = 4n^2 + 4n + 1$ as $c \neq 1$. Finally assume that $p = 2n$ and $q \geq 2n + 3$,

$$4n^2 + 6n = (2n)(2n + 3) \leq pq = F(n) = 4n^2 + 4n + c \implies 2n \leq c$$

and is a contradiction for $n > c$. Finally take $q = 2n + 2$ to get the contradiction $4n^2 + 4n = (2n)(2n + 2) = pq \neq F(n) = 4n^2 + 4n + c$. Therefore if the recursively factorable criterion holds for the values in the interval $[-c, c]$, then $2n > p$ and the criterion holds for the values outside of the interval also. \square

Remark 3.6. With some additional casework to show that the values over a suitably large interval satisfy the recursively-factorable criterion, it can also be shown that the polynomials in Table 1 are recursively-factorable. Some of these quadratics are prime-producing polynomials, or a horizontal shift of one, listed in [22] and [30].

For these real-root quadratics, the condition $|F(m)| < |F(n)|$ for $m \in [2 - n, n - 1]$ no longer holds as it did in Lemma 3.5. However for $n > \max \left\{ \frac{-b - \sqrt{b^2 + 8ac}}{2a}, \frac{-b + \sqrt{b^2 + 8ac}}{2a} \right\}$, $|F(m)| < |F(n)|$

for all $m \in (-n - \frac{b}{a}, n)$. Hence \hat{n} can be chosen to be sufficiently large so that, for all $n > \hat{n}$, both $|F(m)| < |F(n)|$ for $m \in (-n - \frac{b}{a}, n)$ and $\lfloor \sqrt{|F(n)|} \rfloor < |2n + \frac{b}{a}|$.

4. PRESENTATION AS THE PRODUCT OF BINARY QUADRATIC FORMS

We show in this section that, for quadratic polynomials, the factorization presentations of Theorem 2.1, defined recursively as $F(\sum_{k=1}^m x_k f_{k-1}) = f_{m-1} f_m$, may be expressed in a closed form as the product of two binary quadratic forms. Theorem 4.6 establishes that, in this context, each factorization presentation sequence (x_1, \dots, x_m) corresponds with a particular $A_m \in M_2(\mathbb{Z})$.

Definition 4.1. Fix $F(n) = a n^2 + b n + c$. Let $\Delta_F, \eta_F, \phi_{F,0}$, and $\phi_{F,1}$ be functions from $M_2(\mathbb{Z}) \rightarrow \mathbb{Z}$ defined such that for $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$,

$$(9) \quad \begin{aligned} \Delta_F[A] &= \alpha \delta - a \beta \gamma, \\ \eta_F[A] &= \alpha \gamma + b \beta \gamma + c \beta \delta, \\ \phi_{F,0}[A] &= \alpha^2 + b \alpha \beta + a c \beta^2, \\ \phi_{F,1}[A] &= a \gamma^2 + b \gamma \delta + c \delta^2, \end{aligned}$$

and for natural m ,

$$(10) \quad \phi_{F,m}[A] = \begin{cases} \phi_{F,0}[A] & \text{for even } m \\ \phi_{F,1}[A] & \text{for odd } m \end{cases}.$$

We suppress the F when it is clear by the context, favoring the notation $\Delta[A], \eta[A], \phi_0[A], \phi_1[A]$, and $\phi_m[A]$.

Definition 4.2. For $a \in \mathbb{Z}$, let

$$(11) \quad \Gamma_a := \{A \in M_2(\mathbb{Z}) : \Delta[A] = 1\}.$$

In general, the set Γ_a is not closed under matrix multiplication and does not contain its inverses. However the case when $a = 1$ is particularly noteworthy as $\Gamma_1 = \text{SL}_2(\mathbb{Z})$ is the special linear group.

Theorem 4.3. Let $F : \mathbb{Z} \rightarrow \mathbb{Z}$ such that $F(x) = a x^2 + b x + c$. For $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$,

$$F(\alpha \gamma + b \beta \gamma + c \beta \delta) = (\alpha^2 + b \alpha \beta + a c \beta^2)(a \gamma^2 + b \gamma \delta + c \delta^2)$$

if and only if $\alpha \delta - a \beta \gamma = 1$ or $-1 - \frac{b(\alpha \gamma + b \beta \gamma + c \beta \delta)}{c}$, i.e., for $A \in M_2(\mathbb{Z})$,

$$(12) \quad F(\eta[A]) = \phi_0[A] \phi_1[A]$$

if and only if $\Delta[A] = 1$ or $-1 - \frac{b}{c} \eta[A]$.

Proof. By expanding both sides, one can verify that:

$$\begin{aligned} &F(\alpha \gamma + b \beta \gamma + c \beta \delta) - (\alpha^2 + b \alpha \beta + a c \beta^2)(a \gamma^2 + b \gamma \delta + c \delta^2) \\ &= (1 - (\alpha \delta - a \beta \gamma))(c(\alpha \delta - a \beta \gamma) + (c + b(\alpha \gamma + b \beta \gamma + c \beta \delta))). \end{aligned}$$

□

Remark 4.4. The set of matrices $\mathcal{K}_1 \subset \Gamma_a$ given by

$$(13) \quad \mathcal{K}_1 = \left\{ \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ s & -1 \end{pmatrix} \right\},$$

$\mathcal{K}_2 \subset \Gamma_1$ and $\mathcal{K}_3 \subset \Gamma_{-1}$ given by

$$(14) \quad \mathcal{K}_2 = \left\{ \begin{pmatrix} s & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} s & -1 \\ 1 & 0 \end{pmatrix} \right\} \quad \text{and} \quad \mathcal{K}_3 = \left\{ \begin{pmatrix} s & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} s & -1 \\ -1 & 0 \end{pmatrix} \right\},$$

respectively, correspond to the trivial factorization in Theorem 4.3 for each $s \in \mathbb{Z}$.

The Fibonacci-Brahmagupta identity has a long history in mathematics beginning with its first appearance in Diophantus' *Arithmetica* (III, 19) [8] c.250 in the form of $(p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2$. Later in c.628, Brahmagupta generalized Diophantus' identity by showing that numbers of the form $p^2 + cq^2$ are closed under multiplication. Brahmagupta's identity was popularized in 1225 upon its reprinting in Fibonacci's *Liber Quadratorum* [11] where the first rigorous proof of the identity appeared. Finally in 1770, Euler [9] further generalized Brahmagupta's identity by providing the parametric solution

$$(15) \quad (adp^2 + ceq^2)(der^2 + acs^2) = ae(dpr \pm cqs)^2 + cd(aps \mp eqr)^2$$

for the Diophantine equation $Ax^2 + By^2 = C$ with composite C . In Corollary 4.5 we show that the case $b = 0$ in Theorem 4.3 corresponds to the case $d = e = 1$ in Euler's Identity (15).

Corollary 4.5.

$$a(\alpha\gamma + c\beta\delta)^2 + c(\alpha\delta - a\beta\gamma)^2 = (\alpha^2 + ac\beta^2)(a\gamma^2 + c\delta^2)$$

Proof. When $b = 0$, $F(x) = ax^2 + c$ and

$$\begin{aligned} a(\alpha\gamma + c\beta\delta)^2 + c \cdot 1^2 &= F(\alpha\gamma + c\beta\delta) \\ &= (\alpha^2 + ac\beta^2)(a\gamma^2 + c\delta^2) \end{aligned}$$

where $\alpha\delta - a\beta\gamma = 1$. Hence

$$a(\alpha\gamma + c\beta\delta)^2 + c(\alpha\delta - a\beta\gamma)^2 = (\alpha^2 + ac\beta^2)(a\gamma^2 + c\delta^2). \quad \square$$

Theorem 4.6. For $F(n) = an^2 + bn + c$ and $m \geq 0$,

$$f_m(x_1, \dots, x_m) = \phi_m[A_m]$$

where $A_m \in \Gamma_a$ defined recursively by

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A_{k+1} = \begin{pmatrix} \alpha_{k+1} & \beta_{k+1} \\ \gamma_{k+1} & \delta_{k+1} \end{pmatrix} = A_k + x_{k+1}B_k$$

for $1 \leq k \leq m-1$ such that

$$B_k = \begin{cases} \begin{pmatrix} a\gamma_k & \delta_k \\ 0 & 0 \end{pmatrix} & \text{for odd } k \\ \begin{pmatrix} 0 & 0 \\ \alpha_k & a\beta_k \end{pmatrix} & \text{for even } k \end{cases}.$$

Proof. We shall proceed by induction on m . For each $1 \leq k \leq m$, define $A_k \in \Gamma_a$ and B_k recursively as stated in the hypothesis. Initially we see that $f_0 = 1 = \phi_0[A_0]$ and $f_1 = F(x_1) = \phi_1[A_1]$ satisfies the hypothesis. Now assume $f_{2j} = \phi_0[A_{2j}]$ and $f_{2j+1} = \phi_1[A_{2j+1}]$ for each $0 \leq j \leq \lceil \frac{m}{2} \rceil$. Suppose $m = 2j$ for some $j \geq 1$. Remark 2.2 gives

$$(16) \quad f_{2j} = f_{2j-2} + x_{2j} \frac{\partial}{\partial x_{2j-1}} [f_{2j-1}] + ax_{2j}^2 f_{2j-1}.$$

By the induction hypothesis

$$(17) \quad f_{2j-2} = \phi_0[A_{2j-2}] = \alpha_{2j-2}^2 + b \alpha_{2j-2} \beta_{2j-2} + ac \beta_{2j-2}^2$$

and

$$(18) \quad f_{2j-1} = \phi_1[A_{2j-1}] = a \gamma_{2j-1}^2 + b \gamma_{2j-1} \delta_{2j-1} + c \delta_{2j-1}^2.$$

The partial derivative $\frac{\partial}{\partial x_{2j-1}} [\phi_1[A_{2j-1}]]$ may be evaluated through the equation $A_{2j-1} = A_{2j-2} + x_{2j-1} B_{2j-2}$. In particular

$$\frac{\partial}{\partial x_{2j-1}} [\gamma_{2j-1}] = \alpha_{2j-2} \quad \text{and} \quad \frac{\partial}{\partial x_{2j-1}} [\delta_{2j-1}] = a \beta_{2j-2}$$

which yields

$$(19) \quad \begin{aligned} \frac{\partial}{\partial x_{2j-1}} [f_{2j-1}] &= \frac{\partial}{\partial x_{2j-1}} [\phi_1[A_{2j-1}]] \\ &= \frac{\partial}{\partial x_{2j-1}} [a \gamma_{2j-1}^2 + b \gamma_{2j-1} \delta_{2j-1} + c \delta_{2j-1}^2] \\ &= 2a \gamma_{2j-1} \alpha_{2j-2} + b (a \gamma_{2j-1} \beta_{2j-2} + \delta_{2j-1} \alpha_{2j-2}) + 2ac \delta_{2j-1} \beta_{2j-2} \end{aligned}$$

Substituting (17), (18), and (19) into (16) gives

$$(20) \quad \begin{aligned} f_{2j} &= (\alpha_{2j-2}^2 + b \alpha_{2j-2} \beta_{2j-2} + ac \beta_{2j-2}^2) \\ &\quad + x_{2j} (2a \gamma_{2j-1} \alpha_{2j-2} + ab \gamma_{2j-1} \beta_{2j-2} + b \delta_{2j-1} \alpha_{2j-2} \\ &\quad + 2ac \delta_{2j-1} \beta_{2j-2}) + x_{2j}^2 (a (a \gamma_{2j-1}^2 + b \gamma_{2j-1} \delta_{2j-1} + c \delta_{2j-1}^2)). \end{aligned}$$

As defined in the hypothesis,

$$(21) \quad \begin{aligned} A_{2j} &= A_{2j-1} + x_{2j} B_{2j-1} \\ &= (A_{2j-2} + x_{2j-1} B_{2j-2}) + x_{2j} B_{2j-1} \\ &= \begin{pmatrix} \alpha_{2j-2} & \beta_{2j-2} \\ \gamma_{2j-2} & \delta_{2j-2} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ x_{2j-1} \alpha_{2j-2} & a x_{2j-1} \beta_{2j-2} \end{pmatrix} + \begin{pmatrix} a x_{2j} \gamma_{2j-1} & x_{2j} \delta_{2j-1} \\ 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} \alpha_{2j-2} + a x_{2j} \gamma_{2j-1} & \beta_{2j-2} + x_{2j} \delta_{2j-1} \\ \gamma_{2j-2} + x_{2j-1} \alpha_{2j-2} & \delta_{2j-2} + a x_{2j-1} \beta_{2j-2} \end{pmatrix} \end{aligned}$$

so

$$(22) \quad \begin{aligned} \phi_{2j}[A_{2j}] &= \phi_0[A_{2j}] \\ &= (\alpha_{2j-2} + a x_{2j} \gamma_{2j-1})^2 + ac (\beta_{2j-2} + x_{2j} \delta_{2j-1})^2 \\ &\quad + b (\alpha_{2j-2} + a x_{2j} \gamma_{2j-1}) (\beta_{2j-2} + x_{2j} \delta_{2j-1}). \end{aligned}$$

Comparing (20) and (22) shows that $f_{2j} = \phi_{2j}[A_{2j}]$.

Initially $\Delta[A_0] = 1$ and by the induction hypothesis $\Delta[A_k] = 1$ for $1 \leq k \leq m-1$, so we check that $A_m \in \Gamma_a$:

$$\begin{aligned} \Delta[A_m] &= \Delta \left[\begin{pmatrix} \alpha_{m-1} + x_m a \gamma_{m-1} & \beta_{m-1} + x_m \delta_{m-1} \\ \gamma_{m-1} & \delta_{m-1} \end{pmatrix} \right] \\ &= (\alpha_{m-1} + x_m a \gamma_{m-1}) \delta_{m-1} - a (\beta_{m-1} + x_m \delta_{m-1}) \gamma_{m-1} \\ &= (\alpha_{m-1} \delta_{m-1} - a \beta_{m-1} \gamma_{m-1}) = \Delta[A_{m-1}] = 1. \end{aligned}$$

Similarly when $m = 2j + 1$, Remark 2.2 says that

$$(23) \quad f_{2j+1} = f_{2j-1} + x_{2j+1} \frac{\partial}{\partial x_{2j}} [f_{2j}] + a x_{2j+1}^2 f_{2j}.$$

whose partial derivative $\frac{\partial}{\partial x_{2j}} [f_{2j}] = \frac{\partial}{\partial x_{2j}} [\phi_{2j}[A_{2j}]]$ may be computed through (22) as

$$(24) \quad \frac{\partial}{\partial x_{2j}} [f_{2j}] = 2a\alpha_{2j}\gamma_{2j-1} + b\alpha_{2j}\delta_{2j-1} + ab\gamma_{2j-1}\beta_{2j} + 2ac\beta_{2j}\delta_{2j-1}$$

since $\alpha_{2j} = \alpha_{2j-2} + ax_{2j}\gamma_{2j-1}$ and $\beta_{2j} = \beta_{2j-2} + x_{2j}\delta_{2j-1}$. Putting (18), (23), and (24) together with the fact that $f_{2j} = \phi_0[A_{2j}]$ gives

$$(25) \quad \begin{aligned} f_{2j+1} = & (a\gamma_{2j-1}^2 + b\gamma_{2j-1}\delta_{2j-1} + c\delta_{2j-1}^2) \\ & + x_{2j+1}(2a\alpha_{2j}\gamma_{2j-1} + b\alpha_{2j}\delta_{2j-1} + ab\gamma_{2j-1}\beta_{2j} \\ & + 2ac\beta_{2j}\delta_{2j-1}) + x_{2j+1}^2(a(\alpha_{2j}^2 + b\alpha_{2j}\beta_{2j} + ac\beta_{2j}^2) \end{aligned}$$

and may be compared with $\phi_{2j+1}[A_{2j+1}]$ which is computed thusly:

$$(26) \quad \begin{aligned} \phi_{2j+1}[A_{2j+1}] = & \phi_1 \left[\begin{pmatrix} \alpha_{2j-1} + ax_{2j}\gamma_{2j-1} & \beta_{2j-1} + x_{2j}\delta_{2j-1} \\ \gamma_{2j-1} + x_{2j+1}\alpha_{2j} & \delta_{2j-1} + ax_{2j+1}\beta_{2j} \end{pmatrix} \right] \\ = & a(\gamma_{2j-1} + x_{2j+1}\alpha_{2j})^2 + c(\delta_{2j-1} + ax_{2j+1}\beta_{2j})^2 \\ & + b(\gamma_{2j-1} + x_{2j+1}\alpha_{2j})(\delta_{2j-1} + ax_{2j+1}\beta_{2j}). \end{aligned}$$

Checking that (25) is equal to (26) shows $f_m = \phi_m[A_m]$.

We have that $\Delta[A_k] = 1$ for $1 \leq k \leq m-1$, so

$$\begin{aligned} \Delta[A_m] = & \Delta \left[\begin{pmatrix} \alpha_{m-1} & \beta_{m-1} \\ \gamma_{m-1} + x_m\alpha_{m-1} & \delta_{m-1} + x_m a\beta_{m-1} \end{pmatrix} \right] \\ = & \alpha_{m-1}(\delta_{m-1} + x_m a\beta_{m-1}) - a\beta_{m-1}(\gamma_{m-1} + x_m\alpha_{m-1}) \\ = & (\alpha_{m-1}\delta_{m-1} - a\beta_{m-1}\gamma_{m-1}) = \Delta[A_{m-1}] = 1. \end{aligned}$$

which completes the proof. \square

Combining Theorems 3.4 and 4.6 implies that for a recursively-factorable polynomial F , each non-trivial factorization presentation $(n, p, q \in \mathbb{Z} : |F(n)| = pq)$ is represented by some $A_m \in \Gamma_a$ via the identity $F(\eta[A_m]) = \phi_0[A_m]\phi_1[A_m]$ from Theorem 4.3.

Example 4.7. Returning to Example 2.4, for $F(n) = 3n^2 + 5n + 11$ we can compute $f_3(2, -1, 4)$ using Theorem 4.6:

$$\begin{aligned} A_1 &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \\ A_2 &= \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} + (-1) \begin{pmatrix} 3 \cdot 2 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -5 & -1 \\ 2 & 1 \end{pmatrix} \\ A_3 &= \begin{pmatrix} -5 & -1 \\ 2 & 1 \end{pmatrix} + (4) \begin{pmatrix} 0 & 0 \\ -5 & 3 \cdot (-1) \end{pmatrix} = \begin{pmatrix} -5 & -1 \\ -18 & -11 \end{pmatrix} \end{aligned}$$

and

$$f_3(2, -1, 4) = \phi_1[A_3] = 3(-18)^2 + 5(-18)(-11) + 11(-11)^2 = 3293.$$

It is readily checked that $\Delta[A_3] = 1$ and meets the conditions of Theorem 4.3. Since $\eta[A_3] = 301$ and $\phi_2[A_3] = 83$, it follows that

$$F(301) = 3293 \times 83.$$

Remark 4.8. The non-trivial factorization $F(1) = 3 \cdot 3$, but $F(0) = 7$ is the only value less than $F(1)$ and $1 \not\equiv 0 \pmod{3}$. Likewise $F(1) = 3 \cdot 3$ cannot be represented by Theorem 4.3, since 3 cannot be represented by the binary form $\phi_0[A] = \alpha^2 + \alpha\beta + 7\beta^2$, see [5] for more details.

Remark 4.9. Recall that the special linear group may be generated by its transvections [14]. In particular, $\text{SL}_2(\mathbb{Z}) = \langle T, U \rangle$ where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. It follows that

$$T^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad U^i = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$$

for all $i \in \mathbb{Z}$.

Corollary 4.10. For $F(n) = n^2 + bn + c$,

$$(27) \quad f_m(x_1, x_2, \dots, x_{2i-1}, x_{2i}, \dots, x_m) = \phi_m[W^{x_m} \dots T^{x_{2i}} U^{x_{2i-1}} \dots T^{x_2} U^{x_1}]$$

where $W = \begin{cases} U, & \text{if } m \text{ is odd} \\ T, & \text{if } m \text{ is even.} \end{cases}$

Proof. From Theorem 4.6, $f_m = \phi_m[A_m]$ where $A_0 = I$ and

$$(28) \quad A_k = \begin{cases} \begin{pmatrix} \alpha_{k-1} & \beta_{k-1} \\ \gamma_{k-1} + x_k \alpha_{k-1} & \delta_{k-1} + x_k \beta_{k-1} \end{pmatrix} = U^{x_k} A_{k-1} & \text{for odd } k \\ \begin{pmatrix} \alpha_{k-1} + x_k \gamma_{k-1} & \beta_{k-1} + x_k \delta_{k-1} \\ \gamma_{k-1} & \delta_{k-1} \end{pmatrix} = T^{x_k} A_{k-1} & \text{for even } k \end{cases}$$

for each $1 \leq k \leq m$. □

It stands to reason that shifting a polynomial horizontally does not change the integer factorization of its values. In the case of quadratics, the specific correspondence between a parabola and its shift is expressed by the following proposition.

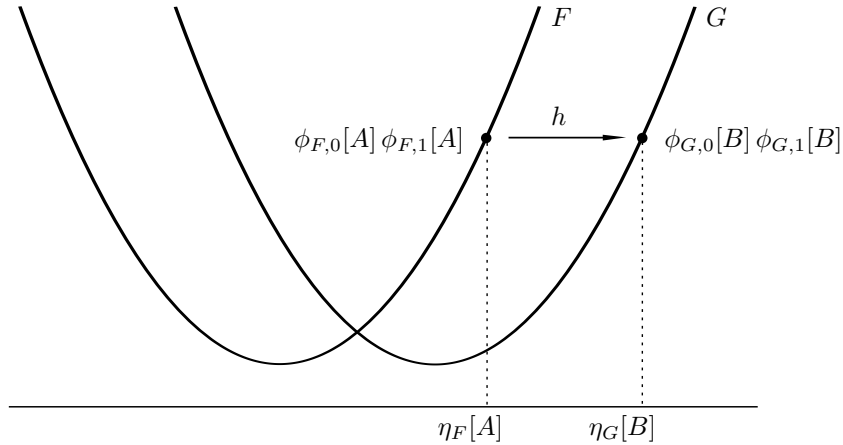


FIGURE 3. Correspondence between integer factorizations for shifted parabolas.

Proposition 4.11. Let $F(n) = an^2 + bn + c$ and set $G(n) = F(n - h)$ for some $h \in \mathbb{Z}$. For each $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_a$ there is a corresponding

$$B = A + h \begin{pmatrix} a\beta & 0 \\ \delta & 0 \end{pmatrix}$$

for which the following conditions hold:

- (i) $B \in \Gamma_a$,
- (ii) $\eta_G[B] = \eta_F[A] + h$,
- (iii) $\phi_{G,0}[B] = \phi_{F,0}[A]$, and
- (iv) $\phi_{G,1}[B] = \phi_{F,1}[A]$.

Proof. Let $B = \begin{pmatrix} \alpha + ha\beta & \beta \\ \gamma + h\delta & \delta \end{pmatrix}$ such that $\alpha\delta - a\beta\gamma = 1$. Noting that

$$G(n) = F(n - h) = an^2 + (b - 2ah)n + (c - bh + ah^2) :$$

- (i) $\Delta_G[B] = (\alpha + ha\beta)\delta - a\beta(\gamma + h\delta)$
 $= \alpha\delta - a\beta\gamma = 1.$
- (ii) $\eta_G[B] = (\alpha + ha\beta)(\gamma + h\delta) + (b - 2ah)\beta(\gamma + h\delta) + (c - bh + ah^2)\beta\delta$
 $= (\alpha\gamma + b\beta\gamma + c\beta\delta) + h(\alpha\delta - a\beta\gamma)$
 $= \eta_F[A] + h.$
- (iii) $\phi_{G,1}[B] = a(\gamma + h\delta)^2 + (b - 2ah)(\gamma + h\delta)\delta + (c - bh + ah^2)\delta^2$
 $= a\gamma^2 + b\gamma\delta + c\delta^2.$
- (iv) $\phi_{G,2}[B] = (\alpha + ha\beta)^2 + (b - 2ah)(\alpha + ha\beta)\beta + a(c - bh + ah^2)\beta^2$
 $= \alpha^2 + b\alpha\beta + ac\beta^2. \quad \square$

5. LATTICE POINTS ON THE CONIC SECTION $aX^2 + bXY + cY^2 + X - nY = 0$

Lastly, Theorem 5.1 relates the set Γ_a with the lattice point solutions of the conic sections $aX^2 + bXY + cY^2 + X - nY = 0$. From Theorem 4.3, each $A_m \in \Gamma_a$ corresponds to an integer factorization presentation of a value of $F(n) = an^2 + bn + c$, i.e., the problem of finding lattice point solutions to these conic sections is equivalent to factoring the value of an associated quadratic polynomial.

Theorem 5.1. For $a, b, c \in \mathbb{Z}$, let

$$\mathcal{L}_a = \{(X, Y) \in \mathbb{Z}^2 \mid aX^2 + bXY + cY^2 + X - nY = 0 \text{ for any } n \in \mathbb{N}\}$$

The map $\psi : \Gamma_a / \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3 \rightarrow \mathcal{L}_a / \{(0, 0), (-1, 0), (1, 0)\}$ defined by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \beta\gamma \\ \beta\delta \end{pmatrix}$$

is a bijection.

Proof. Fix $a, b, c \in \mathbb{Z}$ and consider $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_a$. Set $n = \eta[A]$, $X = \beta\gamma$, $Y = \beta\delta$, and $Z = \alpha\gamma$. Direct substitution shows that

$$(29) \quad Z + bX + cY = \alpha\gamma + b\beta\gamma + c\beta\delta = \eta[A] = n.$$

Since $A \in \Gamma_a$, it follows that $\Delta[A] = 1$ and $\beta\gamma(\alpha\delta - a\beta\gamma) = \beta\gamma(1)$, i.e.,

$$(30) \quad ZY = X + aX^2.$$

Solving for Z in (29) and substituting it into (30) shows that (X, Y) is a solution to

$$(31) \quad aX^2 + bXY + cY^2 + X - nY = 0.$$

Now consider the inverse map $\psi^{-1} : \mathcal{L}_a / \{(0, 0), (-1, 0), (1, 0)\} \rightarrow \Gamma_a / \mathcal{K}_1 \cup \mathcal{K}_2 \cup \mathcal{K}_3$ defined by

$$(32) \quad \begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} \frac{\gcd(X, Y)}{Y}(1 + aX) & \gcd(X, Y) \\ \frac{X}{\gcd(X, Y)} & \frac{Y}{\gcd(X, Y)} \end{pmatrix}.$$

For each $L = (X, Y) \in \mathcal{L}_a$, $\Delta[\psi^{-1}(L)] = 1$ and from (31)

$$X(1 + aX) = Y(n - bX - cY)$$

so $\frac{\gcd(X, Y)}{Y}(1 + aX) \in \mathbb{Z}$. Hence $\psi^{-1}(L) \in \Gamma_a$.

We show that ψ is injective by verifying that $\psi^{-1} \circ \psi(A) = A$ for each $A \in \Gamma_a$. Indeed, since $\Delta[A] = 1$ the $\gcd(\alpha\delta, a\beta\gamma) = 1$ implying that $\gcd(\gamma, \delta) = 1$, i.e., $\gcd(\beta\gamma, \beta\delta) = \beta$. Thus,

$$\psi^{-1}\psi[A] = \psi^{-1} \left[\begin{pmatrix} \beta\gamma \\ \beta\delta \end{pmatrix} \right] = \begin{pmatrix} \frac{\beta}{\beta\delta}(1 + a\beta\gamma) & \frac{\beta}{\beta\delta} \\ \frac{\beta\gamma}{\beta} & \frac{\beta\delta}{\beta} \end{pmatrix} = A$$

since $\Delta[A] = 1$ implies that $\alpha = \frac{1}{\delta}(1 + a\beta\gamma)$.

Likewise, for each $(X, Y) \in \mathcal{L}_a$,

$$\psi \circ \psi^{-1} \left[\begin{pmatrix} X \\ Y \end{pmatrix} \right] = \psi \left[\begin{pmatrix} \frac{G}{Y}(1 + aX) & G \\ \frac{X}{G} & \frac{Y}{G} \end{pmatrix} \right] = \begin{pmatrix} X \\ Y \end{pmatrix}$$

meaning ψ is surjective. \square

The mapping $\psi : \mathcal{K}_1 \mapsto \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ defined by $\psi \left[\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right] = \begin{pmatrix} \beta\gamma \\ \beta\delta \end{pmatrix}$ is well-defined and onto, but is not one-to-one. Similarly, when $a = 1$ or -1 the respective mappings $\psi : \mathcal{K}_2 \mapsto \begin{pmatrix} -1 \\ 0 \end{pmatrix}$ and $\psi : \mathcal{K}_3 \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ are onto but not one-to-one. Therefore the image of ψ under Γ_a is \mathcal{L}_a .

Example 5.2. Consider the Euler-like polynomial $F(n) = n^2 - n + 5$. It is easy to verify that $(X, Y) = (3, 4)$ is a solution of

$$(33) \quad X^2 - XY + 5Y^2 + X - 20Y = 0.$$

By Theorem 5.1, the point $(3, 4)$ corresponds to the element $A \in \Gamma_1$ given by

$$A = \psi^{-1} \left[\begin{pmatrix} 3 \\ 4 \end{pmatrix} \right] = \begin{pmatrix} 1 & 1 \\ 3 & 4 \end{pmatrix}.$$

Thus $F(\eta[A]) = F(20) = 5 \cdot 77 = \phi_1[A]\phi_2[A]$. Similarly $(0, 0)$, $(5, 2)$, $(5, 3)$, $(0, 4)$, $(-3, 3)$, $(-4, 2)$ and $(-1, 0)$ are also lattice point solutions (see Figure 4) to (33) corresponding to the integer factorizations $1 \cdot 385$, $11 \cdot 35$, $7 \cdot 55$, $77 \cdot 5$, $55 \cdot 7$, $35 \cdot 11$, and $385 \cdot 1$, respectively.

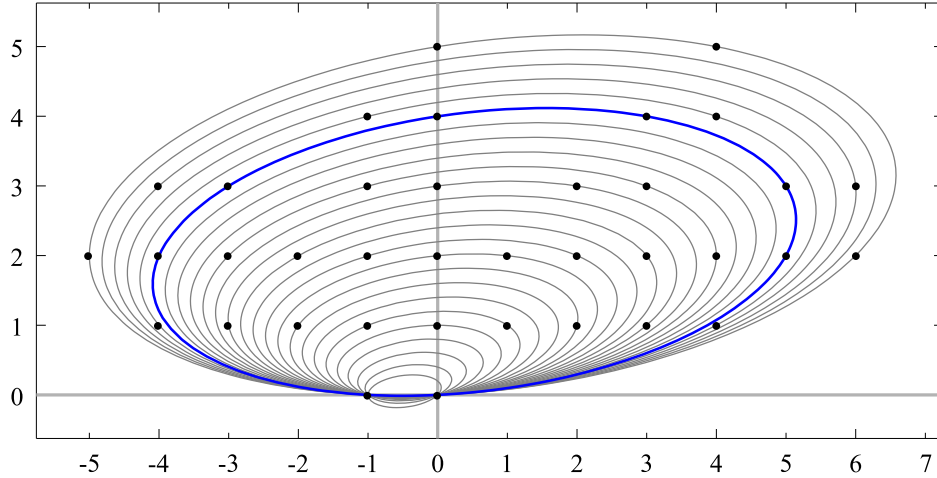


FIGURE 4. Plot of $X^2 - XY + 5Y^2 + X - nY = 0$ for $n = 0, \dots, 25$. The case $n = 20$ is highlighted in blue and lattice points $(X, Y) \in \mathcal{L}_1$ intersecting the ellipses are indicated.

Remark 5.3. Gauss [23, 13] showed that the general binary quadratic Diophantine equation can be reduced to a special case of the Pell equation. In particular, (31) can be reduced to

$$(34) \quad U^2 - (b^2 - 4ac)V^2 = 4a(an^2 + bn + c)$$

where $U = (b^2 - 4ac)Y + (b + 2an)$ and $V = 2aX + bY + 1$ provided that $b^2 - 4ac \neq 0$. The trivial factorization $F(n) = 1 \cdot F(n)$ corresponds to the solution $U = \pm(2an + b)$ and $V = \pm 1$.

6. ACKNOWLEDGEMENTS

I would like to thank John Quintanilla and Nataša Jonoska for their useful discussions.

REFERENCES

- [1] Atkin, A. O. L., Bernstein, D. J., “Prime Sieves Using Binary Quadratic Forms,” *Mathematics of Computation*. **7**:246 (2003), pp. 1023-1030.
- [2] Baker, A. “Imaginary Quadratic Fields with Class Number Two,” *Ann. Math.* **94** (1971), pp. 139-152.
- [3] Brahmagupta, *Brâhma-sphuta-siddhânta* (628).
- [4] Bouniakowsky, V. “Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs,” *Mém. Acad. Sc. St. Pétersbourg*, **6** (1857). pp. 305-329.
- [5] Conway, J. H. *The Sensual (Quadratic) Form*. Carus Mathematical Monographs **26**, Mathematical Association of America, Washington, DC (1997).
- [6] Crandall, R., Pomerance, C., *Prime numbers. A computational perspective*, New York: Springer-Verlag (2001).
- [7] Dickson, L. *History of the Theory of Numbers: Quadratic and Higher Forms*, Volume III. Chelsea Publishing Company, New York (1971).
- [8] Diophantus, *Arithmetica: Book III*, Problem 19 (c. 250).
- [9] Euler, L. *Algebra*, St. Petersburg, 2 (1770). Ch.11 §§173-180
- [10] Euler, L. Extrait d’une lettre de M. Euler le père à M. Bernoulli concernant le memoire imprimé parmi ceux de 1771, *Nouveaux mémoires de l’Académie des Sciences de Berlin* 1772 (1774), p. 381
- [11] Fibonacci, *Liber Quadratorum*, (1225).
- [12] Frobenius, “Über quadratische Formen, die viele Primzahlen darstellen,” *Sitzungsber. d. Kgl. Preuß. Akad. Wiss. zu Berlin*, (1912), pp. 966-980. Reprinted in *Gesammelte Abhandlungen*, Vol. III, 573-587. Springer-Verlag, Berlin. (1968).

- [13] Gauss, C. F., tr. Clarke, A. A., *Disquisitiones Arithmeticae*, Yale University Press, (1965).
- [14] Hahn, A. J., O'Meara, O. T., *The Classical Groups and K-Theory*, Springer, New York, (1989).
- [15] Hardy, G. H., Littlewood, J. E., "Partitio numerorum III: On the expression of a number as a sum of primes," *Acta Math.*, **44**, (1923), pp. 1-70.
- [16] Hardy, K., Muskat, J.B., Williams, K.S., "A Deterministic Algorithm for Solving $n = fu^2 + gv^2$ in Coprime Integers u and v ," *Math. of Comp.* **55**:191 (1990), pp. 327-343.
- [17] Heegner, K. "Diophantische Analysis und Modulfunktionen," *Math. Z.* **56** (1952), pp. 227-253.
- [18] Landau, E., "Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion," *Proc. of the Fifth Internat. Congr. of Math.*, Cambridge, Aug. 22-28, 1912, **1** (1913), pp. 93-108.
- [19] Legendre, A. M. *Théorie des nombres*, Librairie Scientifique, A. Herman, Paris (1798). 69-76; second ed. (1808); third ed. (1830), pp. 72-80.
- [20] Le Lionnais, F. *Les Nombres Remarquables*, Paris: Hermann (1983), pp. 88-144.
- [21] Louboutin, S. "Extensions du théorème de Frobenius-Rabinovitch," *C. R. Acad. Sci. Paris.* **312** (1991), pp. 711-714.
- [22] Mollin, R. A. *Quadratics*, CRC Press, Boca Raton, (1995).
- [23] Mordell, L. *Diophantine Equations*, Academic Press. London (1969).
- [24] Pritchard, P. "Linear prime-number sieves: a family tree," *Sci. Comput. Programming.* **9**:1 (1987), pp. 17-35.
- [25] Rabinowitz, G. "Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern," *Proc. Fifth Internat. Congress Math.* Cambridge **1** (1913), pp. 418-421.
- [26] Ribenboim, P. *The Little Book of Bigger Primes*, Second Edition. Springer-Verlag. New York, NY (1991). ISBN 0-387-97508-X
- [27] Shanks, D. "A Sieve Method for Factoring Number of the Form $n^2 + 1$," *Math. Tables Aids Comput.* **13** (1959), pp. 78-86
- [28] Stark, H. M. "A Complete Determination of the Complex Quadratic Fields of Class Number One," *Michigan Math. J.* **14**, (1967), pp. 1-27.
- [29] Stark, H. M. "A Transcendence Theorem for Class Number Problems," *Ann. Math.* **94** (1971), pp. 153-173.
- [30] Weisstein, E. W. "Prime-Generating Polynomial," From MathWorld—A Wolfram Web Resource. (2014) <http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html>